THE AMENDMENTS

In The Claims:

1. (Currently Amended) A method of controlling access to a network, comprising:

requesting an identity from a mobile client attempting to connect to the network;

receiving the identity;

associating location information corresponding to the client with the identity;

authenticating the identity;

comparing the location information against a policy designating locations, if any, at which the client is permitted to connect to the network;

deciding whether to grant or deny the client access to the network based on the authenticity of the identity and the comparison of the location information;

when access is granted, permitting roaming of the mobile client within the network;

during said roaming, when signal quality from a current access point in communication with the mobile client deteriorates sufficiently, locating another access point;

when another access point is located, associating the mobile client with the newly located access point and allowing the client to continue to access the network upon determining, by comparing updated location information corresponding to the mobile client against the policy, that the mobile client is still authorized to access the network

~~wherein if the client is granted access to the network, and subsequently moves to a new location, the network follows a procedure to either re-authenticate or not re-authenticate the client; and~~

~~wherein if, pursuant to the procedure, the client continues to have access to the network after moving to the new location, the client's access at the new location will be based on policies of the new location~~.

2. (Original) The method of claim 1, further comprising:

passing the identity and the location information to an authentication server, wherein the authentication server performs the steps of authenticating, comparing and deciding.

3. (Currently Amended) The method of claim 2, ~~further comprising the steps of~~ ~~operating~~wherein the authentication server ~~which~~ is a RADIUS server ~~that operates with Steel-Belted Radius, Enterprise Edition;~~

~~wherein RADIUS attributes of an access request packet are defined as type length values (TLVs) that contain additional information,~~

~~wherein vendor specific attributes (VSAs) indicate a vendor ID, and a sting field encoding a sequence of one or more vendor TLVs.~~

4. (Original) The method of claim 1, wherein the identity includes information selected from the group consisting of a user name, a user password, a certificate, a media access control (MAC) address, a shared encryption key, a smart card identifier, and any combination of the foregoing information.

5. (Original) The method of claim 1, wherein the client is a user station capable of connecting to the network through an access point.

6. (Original) The method of claim 1, wherein the client is a wired device capable of connecting to the network through an Ethernet switch port.

7. (Currently Amended) The method of claim 1, comprising:

using a mechanism selected from the group comprising ~~as an authentication mechanism an~~ TLS, TTLS, MD5, EAP-TLS, and any combination of the foregoing ~~protocol~~ to authenticate the identity.

8. (Original) The method of claim 1, wherein the location information indicates the location of a network switch to which the client is attempting to connect.

9. (Original) The method of claim 1, wherein the location information indicates the location of an edge device for connecting the client to the network.

10. (Currently Amended) A network system, comprising:

a network;

an authenticator for requesting an identity from a client and for associating location information corresponding to the client with the identity; ~~and~~

a data structure, accessible by an authentication server, associating identities of clients with their authorized access locations;

~~an~~the authentication server, upon receiving the identity and associated location information from the authenticator, ~~for~~ deciding whether to grant or deny the client access to the network ~~based on the identity and the location information~~ by accessing the data structure and determining that the location information corresponding to the client specifies a location that is one of the authorized access locations, if any, for the client as maintained in the data structure; and

a network manager that allows a network administrator to create and update the data structure

~~wherein if the client is granted access to the network system, and subsequently moves to a new location, the network system follows a procedure to either re-authenticate or not re-authenticate the client; and~~

~~wherein if, pursuant to the procedure, the client continues to have access to network controlled by the network system after moving to the new location, the client's access at the new location will be based on policies of the new location~~.

11. (Original) The network system of claim 10, wherein the authenticator resides in a network switch.

12. (Original) The network system of claim 10, wherein the authenticator resides in an edge device.

13. (Original) The network system of claim 10, further comprising:

an edge device for connecting a user station to a network switch.

14. (Original) The network system of claim 13, wherein the edge device is a wireless access point.

15. (Currently Amended) The network system of claim 14, wherein the user capable of connecting to the network through the access point.

16. (Original) The network system of claim 10, wherein the client is a wired device capable of connecting to a network switch through an Ethernet port.

17. (Original) The network system of claim 10, wherein the location information indicates the location of a network switch to which the client is attempting to connect.

18. (Original) The network system of claim 10, wherein the location information indicates the location of an edge device for connecting the client to the network.

19. (Original) The network system of claim 18, further comprising an interface for permitting an administrator to associate the location information to the edge device.

20. (Original) The network system of claim 10, wherein the authentication server is included in a network switch.

21. (Original) The network system of claim 10, wherein the authentication server authenticates the identity.

22. (Original) The network system of claim 10, wherein the authentication server includes a policy designating locations, if any, at which the client is permitted to connect to the network.

23. (Currently Amended) The network system of claim 10, wherein ~~further comprising,~~

the authentication server is a RADIUS server ~~that operates with Steel-Belted Radius, Enterprise Edition;~~

~~wherein RADIUS attributes of an access request packet are defined as type-length-values (TLVs) that contain additional information; and~~

~~wherein vendor-specific attributes (VSAs) indicate a vendor ID, and a sting field encoding a sequence of one or more vendor~~ TLVs.

24. (Original) The network system of claim 10, wherein the identity includes information selected from the group consisting of a user name, a user password, a certificate, a media access control (MAC) address, a shared key, a smart card identifier, and any combination of the foregoing information.

25. (Currently Amended) The network system of claim 10, further comprising a network switch that comprises:

an authentication mechanism selected from the group consisting of ~~comprising an~~ TLS, TTLS, MD5, EAP-TTLS, EAP-TLS, ~~protocol for authenticating the identity~~and any combination of the foregoing.

26. (Original) The network system of claim 10, wherein the authentication server comprises:

an authentication mechanism selected from the group consisting of TLS, TTLS, MD5, EAP-TTLS, EAP-TLS, and any combination of the foregoing.

27. (Currently Amended) A network system, comprising:

a plurality of edge devices capable of communicating with a plurality of user stations over one or more wireless channels;

a network switch including a plurality of ports for connecting the edge devices to a network;

an application running on the network switch, for requesting station identities from the user stations and for associating corresponding location information with each of the station identities;

a data structure, accessible by an authentication server, associating identities of clients with their authorized access locations;

~~an~~the authentication server ~~for~~ deciding whether to grant or deny each of the user stations access to the network ~~based on the corresponding identity and location information~~ by accessing the data structure and determining, for each user station, that the location information corresponding to the user station specifies a location that is one of the authorized access locations, if any, for the user station as maintained in the data structure; and

a network manager, directly connected to the authentication server, that allows a network administrator to create and update the data structure

~~wherein if the client is granted access to the network system, and subsequently moves to a new location, the network system follows a procedure to either re-authenticate or not re-authenticate the client; and~~

~~wherein if, pursuant to the procedure, the client continues to have access to the network after moving to the new location, the client's access at the new location will be based on policies of the new location~~.

28. (Original) The system of claim 27, wherein at least one of the edge devices is a wireless access point.

29. (Currently Amended) The system of claim 27, ~~wherein at least one of the edge devices is a wireless access point.~~ further comprising a user station that is a wired device for directly connecting one of the ports of the network switch.

30. (Original) The system of claim 27, wherein the location information indicates the location of the network switch.

31. (Original) The system of claim 27, wherein the location information indicates the location of one of the edge devices.

32. (Original) The system of claim 27, wherein the network switch includes an interface for permitting an administrator to associate the location information to the edge devices.

33. (Original) The system of claim 27, wherein the network switch includes an authenticator for authenticating the station identities.

34. (Original) The system of claim 27, wherein the authentication server authenticates the station identities.

35. (Original) The system of claim 27, wherein the authentication server includes a policy designating locations, if any, at which the user stations are permitted to connect to the network.

36. (Currently Amended) The system of claim 27, wherein ~~further comprising,~~

the authentication server is a RADIUS server ~~that operates with Steel-Belted Radius, Enterprise Edition;~~

~~wherein RADIUS attributes of an access request packet are defined as type-length-values (TLVs) that contain additional information; and~~

~~wherein vendor-specific attributes (VSAs) indicate a vendor ID, and a sting field encoding a sequence of one or more vendor~~.

37. (Original) The system of claim 27, wherein the station identities includes information selected from the group consisting of a user name, a user password, a certificate, a media access control (MAC) address, a shared key, a smart card identifier, and any combination of the foregoing information.

38. (Currently Amended) The system of claim 27, further comprising:

an authentication mechanism selected from the group consisting of ~~comprising an~~ TLS,

TTLS, MD5, EAP-TTLS, EAP-TLS, ~~protocol for authenticating the identity~~and any combination of the foregoing.

39. (Currently Amended) A network system for controlling access to a network, comprising:

means for requesting an identity from a mobile client attempting to connect to the network;

means for receiving the identity;

first associating means for associating location information corresponding to the client with the identity;

authenticating means for authenticating the identity;

means for comparing the location information against a policy designating locations, if any, at which the client is permitted to connect to the network;

means for deciding whether to grant or deny the ~~user station~~client access to the network based on the authenticity of the identity and the comparison of the location information, and, when access is granted, permitting roaming of the mobile client within the network;

means for locating another access point upon detecting, during said roaming, when signal quality from a current access point in communication with the mobile client has deteriorated sufficiently;

second associating means for associating the mobile client with the newly located access point and allowing the client to continue to access the network upon determining, by comparing updated location information corresponding to the mobile client against the policy, that the mobile client is still authorized to access the network

~~wherein if the client is granted access to the network system, and subsequently moves to a new location, the network system follows a procedure to either re-authenticate or not re-authenticate the client; and~~

~~wherein if, pursuant to the procedure, the client continues to have access to network controlled by the network system after moving to the new location, the client's access at the new location will be based on policies of the new location~~.

40. (Original) The system of claim 39, wherein the identity includes information selected from the group consisting of a user name, a user password, a certificate, a media access control (MAC) address, a shared key, a smart card identifier, and any combination of the foregoing information.

41. (Original) The system of claim 39, wherein the client is a wireless device capable of connecting to the network through an access point.

42. (Original) The system of claim 39, wherein the client is a wired device capable of connecting to the network through an Ethernet port.

43. (Currently Amended) The system of claim 39, wherein the authenticating means includes:

an authentication mechanism selected from the group consisting of ~~comprising an~~TLS, TTLS, MD5, EAP-TTLS, EAP-TLS, ~~protocol for authenticating the identity~~and any combination of the foregoing.

44. (Original) The system of claim 39, wherein the location information indicates the location of a network switch to which the client is attempting to connect.

45. (Original) The system of claim 39, wherein the location information indicates the location of a edge device for connecting the client to a network switch.

46. (New) The method of claim 1 wherein the mobile client is associated with the newly located access point upon authenticating the identity of the mobile client and determining, by comparing updated location information corresponding to the mobile client against the policy, that the mobile client is still authorized to access the network.

47. (New) The system of claim 39 wherein the second associating means associates the mobile client with the newly located access point upon authenticating the identity of the mobile client and determining, by comparing updated location information corresponding to the mobile client against the policy, that the mobile client is still authorized to access to the network.

48. (New) The method of claim 8, wherein the location information indicates the location of a port of a network switch to which the client is attempting to connect.

49. (New) The network system of claim 17, wherein the location information indicates the location of a port of a network switch to which the client is attempting to connect.

50. (New) The network system of claim 24, wherein the identity includes a smart card identifier.

51. (New) The system of claim 37, wherein the station identities includes a smart card identifier.